PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-191302
(43)Date of publication of application : 21.07.1998

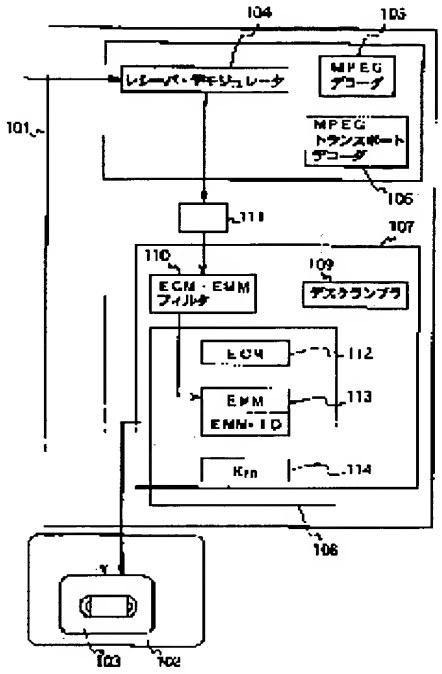
(51)Int.CI. H04N 7/167
H04H 1/00
H04L 9/08
H04L 9/14
H04N 5/91

(21)Application number : 08-351554
(22)Date of filing : 27.12.1996

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : WATANABE KAZUHIRO

(54) DIGITAL SATELLITE BROADCAST RECEIVER

(57)Abstract:
PROBLEM TO BE SOLVED: To allow the user to be able to view a program after descramble even when a long time elapses after the program is recorded by storing separately intermediate key information that is separated from received data, other common key information and scramble program data together with intermediate key ID information.
SOLUTION: EMM(Entitlement Management Message) that is multiplexed on a satellite wave is transmitted. The EMM is extracted and ECM(Entitlement control Message) program data are filtered by an ECM.EMM filter 110 and stored in a program storage means 102. In the case of recording, an EMM-ID corresponding to the EMM is stored in a header area of an ECM program data storage area 113 in the recording. In the case of reproducing recording program data, an IC card 108 selects the EMM to which a matched EMM-ID is assigned from a list in the EMM storage area 113 with the clue of the received EMM-ID.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－191302

(43)公開日　平成10年(1998)７月21日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｎ	7/167		Ｈ０４Ｎ	7/167	Ｚ
Ｈ０４Ｈ	1/00		Ｈ０４Ｈ	1/00	Ｈ
					Ｆ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ
	9/14				６４１

審査請求　未請求　請求項の数22　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平8－351554

(22)出願日　平成８年(1996)12月27日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　渡辺　一裕
大阪府門真市大字門真1006番地　松下電器産業株式会社内

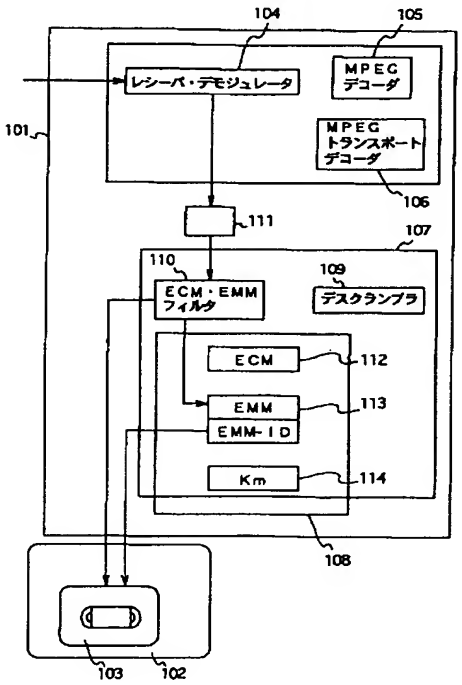
(74)代理人　弁理士　池内　寛幸　（外２名）

(54)【発明の名称】　デジタル衛星放送受信装置

(57)【要約】

【課題】　共通鍵方式の３段階の鍵からデータがスクランブルされたデジタル衛星放送の番組記録およびその再生において、番組を記録した後、長期間が経過して中間鍵が更新された後でもスクランブルを解除することを可能とする。

【解決手段】　ＥＭＭ、ＥＣＭ番組データが多重化された衛星波を受信・復調するレシーバ・デモジュレータ１０４と、マスタ鍵を保持するマスタ鍵記憶手段１１４と、前記受信データをＥＭＭとＥＣＭ・番組データとに分離するＥＣＭ・ＥＭＭフィルタ１１０と、前記ＥＭＭを追記記憶するＥＭＭ記憶手段１１３と、前記ＥＣＭ・番組データ記録手段たる番組記録装置１０２と、前記ＥＣＭ・番組データとそれに対応するＥＭＭとの両者に両者を対応づけるＥＭＭ－ＩＤをそれぞれに割り付けて記録するＥＭＭ－ＩＤ記録手段とを備え、番組データの再生にあたってＥＭＭ－ＩＤを手掛かりに対応するＥＭＭを選択して利用する。



1

【特許請求の範囲】

【請求項１】　装置固有鍵と中間鍵と共通鍵からなる共通鍵暗号方式により番組データをスクランブルし、前記装置固有鍵により暗号化された中間鍵情報と前記中間鍵により暗号化された共通鍵情報と前記共通鍵により暗号化されたスクランブル番組データとを衛星波に多重化して配信するデジタル放送システムに利用されるデジタル衛星放送受信装置において、前記多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を保持する装置固有鍵記憶手段と、前記受信したデータを中間鍵情報と共通鍵情報・スクランブル番組データとに分離する中間鍵情報フィルタと、前記分離した中間鍵情報を記憶する中間鍵情報記憶手段と、前記分離された共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データとそれに対応する中間鍵情報との両者に両者を対応づける中間鍵ＩＤ情報をそれぞれに割り付けて記録する中間鍵ＩＤ情報記録手段とを備えたことを特徴とするデジタル衛星放送受信装置。

【請求項２】　装置固有鍵と中間鍵と共通鍵からなる共通鍵暗号方式により番組データをスクランブルし、前記中間鍵により暗号化された共通鍵情報と前記共通鍵により暗号化されたスクランブル番組データとを衛星波に多重化して配信するデジタル放送システムに利用されるデジタル衛星放送受信装置において、前記装置固有鍵により暗号化された中間鍵情報を受信する手段と、前記多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を記憶する装置固有鍵記憶手段と、前記受信した中間鍵情報を記憶する中間鍵情報記憶手段と、前記受信した共通鍵情報とスクランブル番組データとを記録する共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データとそれに対応する中間鍵情報との両者に両者を対応づける中間鍵ＩＤ情報をそれぞれに割り付けて記録する中間鍵ＩＤ情報記録手段とを備えたことを特徴とするデジタル衛星放送受信装置。

【請求項３】　前記中間鍵情報記憶手段において、中間鍵情報および中間鍵ＩＤ情報の書き込みにあたり現存データに上書きせず追記保存する請求項１または２に記載のデジタル衛星放送受信装置。

【請求項４】　前記記録されている共通鍵情報・スクランブル番組データと中間鍵ＩＤ情報を読み出す記録データ読み出し手段と、前記読み出された中間鍵ＩＤ情報と一致する中間鍵ＩＤ情報に対応付けられて記憶されている中間鍵情報を選択する中間鍵情報選択手段と、前記読み出された共通鍵情報とスクランブル番組データを分離する共通鍵情報フィルタと、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えた請求項１または２に記載のデジタル衛星放送受信装置。

2

【請求項５】　前記中間鍵情報記憶手段において、前記記録する装置が持つ装置固有鍵により復号される中間鍵情報のほか、他の装置に与えられた装置固有鍵により復号される中間鍵情報も併せて記憶する請求項１または２に記載のデジタル衛星放送受信装置。

【請求項６】　装置が装置固有の装置ＩＤ情報を持ち、前記中間鍵情報記憶手段において、前記記憶する中間鍵情報に対応する装置固有鍵を持つ装置の装置ＩＤ情報も併せて記憶する請求項５に記載のデジタル衛星放送受信装置。

【請求項７】　自らの装置ＩＤ情報およびあらかじめ相互利用が設定されている他の装置の装置ＩＤ情報を記憶する手段と、装置が前記中間鍵情報を受信した場合に伴っている装置ＩＤ情報と前記装置内に記憶している装置ＩＤ情報とを比較する装置ＩＤ比較手段と、前記装置ＩＤ比較手段において一致するものがあれば前記中間鍵情報記憶領域に前記中間鍵情報とその対応する装置ＩＤ情報とを合わせて記憶する手段とを備えた請求項６に記載のデジタル衛星放送受信装置。

【請求項８】　前記装置ＩＤ情報と中間鍵ＩＤ情報を手掛かりとして再生・視聴する番組データに対応する中間鍵情報を記憶されている中間鍵ＩＤ情報の中から選択する中間鍵情報選択手段と、前記共通鍵情報とスクランブル番組データとを分離する共通鍵情報・スクランブル番組データ分離手段と、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えた請求項６または７に記載のデジタル衛星放送受信装置。

【請求項９】　装置固有鍵と中間鍵と共通鍵からなる共通鍵暗号方式により番組データをスクランブルし、前記装置固有鍵により暗号化された中間鍵情報と前記中間鍵により暗号化された共通鍵情報と前記共通鍵により暗号化されたスクランブル番組データとを衛星波に多重化して配信するデジタル放送システムに利用されるデジタル衛星放送受信装置において、前記多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を記憶する装置固有鍵記憶手段と、前記受信したデータを中間鍵情報と共通鍵情報・スクランブル番組データとに分離する中間鍵情報フィルタと、前記分離した中間鍵情報を記憶する中間鍵情報記憶手段と、前記分離された共通鍵情報・スクランブル番組データを記録する

3

共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データ記録手段に対して前記記憶されている中間鍵情報を伝達し、共通鍵情報・スクランブル番組データとともに記録する手段とを備えたことを特徴とするデジタル衛星放送受信装置。

【請求項１０】　前記記録されている共通鍵情報・スクランブル番組データと中間鍵情報を読み出す記録データ読み出し手段と、前記読み出された共通鍵情報とスクランブル番組データを分離する共通鍵情報フィルタと、前記装置固有鍵と前記中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えた請求項９に記載のデジタル衛星放送受信装置。

【請求項１１】　前記中間鍵情報記憶手段において、前記記憶する装置が持つ装置固有鍵により復号される中間鍵情報のほか、他の装置に与えられた装置固有鍵により復号される中間鍵情報も併せて記憶する請求項９または１０に記載のデジタル衛星放送受信装置。

【請求項１２】　装置が装置固有の装置ＩＤ情報を持ち、前記中間鍵情報記憶手段において、前記記憶する中間鍵情報に対応する装置固有鍵を持つ装置の装置ＩＤ情報も併せて記憶する請求項１１に記載のデジタル衛星放送受信装置。

【請求項１３】　自らの装置ＩＤ情報およびあらかじめ相互利用が設定されている他の装置の装置ＩＤ情報を記憶する手段と、装置が前記中間鍵情報を受信した場合に伴っている装置ＩＤ情報と前記装置内に記憶している装置ＩＤ情報とを比較する装置ＩＤ情報比較手段と、前記装置ＩＤ情報比較手段において一致するものがあれば前記中間鍵情報記憶領域に前記中間鍵情報とその対応する装置ＩＤ情報とを合わせて記憶する手段とを備えた請求項１２に記載のデジタル衛星放送受信装置。

【請求項１４】　前記装置ＩＤ情報を手掛かりとして再生・視聴する番組データに対応する中間鍵情報を前記記憶されている中間鍵情報の中から選択する中間鍵情報選択手段と、前記共通鍵情報とスクランブル番組データを分離する共通鍵情報・スクランブル番組データ分離手段と、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えた請求項１２または１３に記載のデジタル衛星放送受信装置。

【請求項１５】　前記中間鍵情報および対応する中間鍵

4

ＩＤ情報の記憶領域が、前記装置固有鍵の記憶領域がある記憶媒体と同じ記憶媒体内に設けられている請求項１または２に記載のデジタル衛星放送受信装置。

【請求項１６】　前記記憶媒体がＩＣカードである請求項１５に記載のデジタル衛星放送受信装置。

【請求項１７】　前記中間鍵情報記憶領域が複数の記憶媒体にあり、１つは前記装置固有鍵の記憶領域がある記憶媒体の中に設けられ、他方は前記装置固有鍵の記憶領域がある記憶媒体とは別の記憶媒体に設けられた請求項１または２に記載のデジタル衛星放送受信装置。

【請求項１８】　前記他方の記憶媒体がメモリカードである請求項１７に記載のデジタル衛星放送受信装置。

【請求項１９】　前記共通鍵情報・スクランブル番組データの記録領域が装置に内蔵または外付けで接続された記録媒体にある請求項１，２，９，１０のいずれか１項に記載のデジタル衛星放送受信装置。

【請求項２０】　前記記録媒体が磁気ディスク、内蔵メモリ、またはメモリカードである請求項１９に記載のデジタル衛星放送受信装置。

【請求項２１】　前記共通鍵情報・スクランブル番組データの記録領域が可搬性を持った記録媒体にある請求項１，２，９，１０のいずれか１項に記載のデジタル衛星放送受信装置。

【請求項２２】　前記記録媒体が磁気テープ、光磁気ディスク、ＤＶＤ、ＣＤ－Ｒ、フォトＣＤまたはメモリカードである請求項２１に記載のデジタル衛星放送受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタル衛星放送等のデジタル放送の受信装置に関する。

【０００２】

【従来の技術】近年、衛星を利用したデジタル放送が広がりつつある。デジタル衛星放送では、ＣＡＴＶとは違って番組データは衛星から地上へ向けて放射され、パラボラアンテナなどの電波受信装置があれば誰でも受信できるものであるため、視聴契約など正当に視聴する権利のない者の受信を排除する目的でデータにスクランブルをかけるのが一般的である。また多チャンネル化に伴って複数の放送番組が多重化されてデータが送信されるため、その視聴者が契約した番組のみを視聴させるためにもデータのスクランブルは必要となっている。ここで、スクランブルのセキュリティを高め、視聴者別、番組別の視聴権利の管理のため、共通鍵暗号方式を利用した３重鍵構造の限定受信方式が採用されている。

【０００３】図９および図１０は３重鍵構造の限定受信方式を採用したデジタル放送受信装置およびこれに接続される番組記憶装置の構成を示すものである。図９が番組の録画のときのデータの流れ、図１０が再生のときのデータの流れを示している。暗号鍵として、マスタ鍵

5

（Ｋｍ）、中間鍵たるワーク鍵（Ｋｗ）、番組データのデスクランブルを行なう共通鍵たるスクランブル鍵（Ｋｓ）の３重構造を採用する。ここで前記ワーク鍵Ｋｗをマスタ鍵Ｋｍで暗号化した情報を限定受信個別管理情報（ＥＭＭ：Entitlement Management Message）とし、前記スクランブル鍵をワーク鍵で暗号化したものを限定受信共通情報（ＥＣＭ：Entiltment ControlMessage）とする。

【０００４】図９および図１０において、９０１はデジタル放送受信装置いわゆるセットトップボックス、９０２はデジタルＶＴＲなどの番組記憶装置、９０３は磁気テープなどの記憶媒体、９０４はチューナと復調器から構成される衛星波を受信・復調するレシーバ・デモジュレータ、９０５はＭＰＥＧデコーダ、９０６はＭＰＥＧトランスポートデコーダ、９０７は限定受信を行うためのセキュリティモジュール、９０８はセキュリティモジュール内で限定受信管理を行うＩＣカード、９０９はスクランブルを解除するためのデスクランブラ、９１０はスクランブルを解除するために必要な鍵を含んだ情報である前記限定受信共通情報（ＥＣＭ）および限定受信個別管理情報（ＥＭＭ）をＭＰＥＧトランスポートストリームから選択するためのＥＣＭ・ＥＭＭフィルタ、９１１はＭＰＥＧトランスポートストリーム入力切換回路、９１２はＩＣカード９０８内に格納されているＥＣＭ、９１３はＩＣカード９０８内に格納されているＥＭＭである。

【０００５】３重鍵構造の限定受信方式では、ＭＰＥＧ方式でディジタル圧縮された画像・音声情報をスクランブル鍵Ｋｓにて暗号化する。秘匿性を高めるためスクランブル鍵Ｋｓは１秒程度毎に更新される。スクランブル鍵Ｋｓはワーク鍵Ｋｗにて暗号化され限定受信共通情報ＥＣＭとして、画像・音声情報のデータにＭＰＥＧトランスポート多重化されて伝送される。ワーク鍵Ｋｗは、各ディジタル放送受信装置に固有な鍵であるマスター鍵Ｋｍにて暗号化され限定受信個別管理情報ＥＭＭとして、これもワーク鍵Ｋｗと同様にＭＰＥＧトランスポート多重化されて伝送される。なおマスター鍵Ｋｍは各ディジタル放送受信装置で異なるため、ＥＭＭもそれぞれ異なり、他のディジタル放送受信装置に対応するＥＭＭを使用することはできない。

【０００６】ディジタル放送番組をディジタル情報のままディジタルＶＴＲ等を用いて記録できれば、ディジタル放送の高画質を再生時にも活かすことが可能となる。しかし、映画等の著作権の保護を考慮すると、再生時にも限定受信機能と同じ機能が働くことが望ましい。すなわちスクランブルがかかったままの状態でディジタルＶＴＲ等に記録し、視聴権利を持つディジタル放送受信装置でのみスクランブル解除を可能とする。図９はこのような目的のために構成したディジタル放送受信装置の構成を示すものである。図９では、番組の放送されている

6

時間内のデータをそのまま記録するように構成されており、番組記録装置９０２に対してＥＣＭおよび番組のＭＰＥＧデータを伝送し、記録媒体９０３に記録する。ＥＭＭ９１３は長周期で更新されるため一般にはＩＣカード９０８内に格納されている。

【０００７】

【発明が解決しようとする課題】しかしながら、従来のデジタル衛星放送受信における暗号管理方式および放送番組記録方式においては、番組を記録媒体９０３に記録した後、しばらくは問題なく再生可能であるが、ＥＭＭ９１３が更新された場合、記録された番組に対するワーク鍵Ｋｗが失われることになり、スクランブルを解除することが不可能となる。番組データのスクランブルセキュリティを保つため、前記のように従来例ではスクランブル鍵Ｋｓは１秒ごとという短周期で更新し、ワーク鍵Ｋｗも１か月程度で更新される。つまり視聴者に送信されるＥＣＭおよびＥＭＭが前記周期で更新される。更新後のＥＭＭをマスタ鍵Ｋｍで復号して得られるワーク鍵Ｋｗは、前記放送番組データとともに記録されているＥＣＭには対応していないものであり、前記ワーク鍵Ｋｗで前記記録されているＥＣＭを復号して得られるスクランブル鍵Ｋｓは記録番組データのスクランブル鍵ではない。よって記録した番組データの再生ができなくなってしまうという問題があった。

【０００８】また、複数世帯が同居など視聴者の都合により複数の受信契約があり、複数の受信装置を同時に使用する権利が設定されている場合があるが、記録された番組を他のディジタル放送受信装置を用いて再生する場合においてもワーク鍵Ｋｗもともと相違し、または更新されることにより失われることがあり、スクランブルを解除することが不可能となる可能性があった。

【０００９】本発明は、番組を記録した後、長期間が経過してもスクランブルを解除し視聴することを可能とする方法および、記録に用いたディジタル放送受信装置とは異なる第２のディジタル放送受信装置で再生した場合でも同様にスクランブルを解除し視聴することを可能とする制御ができるデジタル衛星放送受信装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するために本発明に係るデジタル衛星放送受信装置は、多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を保持する装置固有鍵記憶手段と、前記受信したデータを中間鍵情報と共通鍵情報・スクランブル番組データとに分離する中間鍵情報フィルタと、前記分離した中間鍵情報を追記記憶する中間鍵情報記憶手段と、前記分離された共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データとそれに対応する中間鍵情報との両者に両者を対応づける中間鍵ＩＤ情報をそれぞれに割り付けて記録す

る中間鍵ＩＤ情報記録手段とを備える。

【００１１】かかる構成により、本発明に係るデジタル衛星放送受信装置は、多重化されて送られてくるデータから中間鍵情報をその他の共通鍵情報・スクランブル番組データから分離した後に中間鍵ＩＤ情報とともに別途記憶させておくことができ、後日の利用に供することができる。

【００１２】また上記目的を達成するために本発明に係るデジタル衛星放送受信装置は、装置固有鍵により暗号化された中間鍵情報を受信する手段と、前記多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を保持する装置固有鍵記憶手段と、前記受信した中間鍵情報を追記記憶する中間鍵情報記憶手段と、前記受信した共通鍵情報とスクランブル番組データとを記録する共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データとそれに対応する中間鍵情報との両者に両者を対応づける中間鍵ＩＤ情報をそれぞれに割り付けて記録する中間鍵ＩＤ情報記録手段とを備える。

【００１３】かかる構成により本発明に係るデジタル衛星放送受信装置は、中間鍵情報を電話回線などにより受信した場合に受信装置内に中間鍵ＩＤ情報とともに記憶させておくことができ、後日、前記記録されている中間鍵情報の中から、対応付けられている中間鍵ＩＤ情報を手掛かりに記録データに対応する中間鍵を特定して利用することができる。

【００１４】さらに前記デジタル衛星放送受信装置は、前記中間鍵情報記録手段において、前記記録された中間鍵情報は上書きせずに前記中間鍵ＩＤ情報とともに来歴記録として保存することが好ましい。

【００１５】かかる構成により、記録番組データに対応する中間鍵情報が失われることなく、後日記録番組データの視聴にあたって、前記記憶されている中間鍵情報の中から中間鍵ＩＤ情報を基に記録番組データに対応する中間鍵を特定することができる。

【００１６】また上記目的を達成するために本発明に係るデジタル衛星放送受信装置は、前記記録されている共通鍵情報・スクランブル番組データと中間鍵ＩＤ情報を読み出す記録データ読み出し手段と、前記読み出された中間鍵ＩＤ情報と一致する中間鍵ＩＤ情報に対応付けられて記憶されている中間鍵情報を選択する中間鍵情報選択手段と、前記読み出された共通鍵情報とスクランブル番組データを分離する共通鍵情報フィルタと、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備える。

【００１７】かかる構成により、後日の記録番組データの視聴にあたって、中間鍵ＩＤ情報を手掛かりに、再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができ、その中間鍵から得た共通鍵を用いて、記録番組データのスクランブルを解除して再生・視聴することができる。

【００１８】次に前記デジタル衛星放送受信装置は、前記中間鍵情報記憶手段において、前記記録する装置が持つ装置固有鍵により復号される中間鍵情報のほか、他の装置に与えられた装置固有鍵により復号される中間鍵情報も併せて記憶することが好ましい。

【００１９】かかる手段により、視聴権利を持つ複数の装置において、データを相互に再生、視聴するために必要な中間鍵を相互に持つことができる。

【００２０】次に前記デジタル衛星放送受信装置は、装置固有の装置ＩＤ情報を持ち、前記中間鍵情報記憶手段において、前記記憶する中間鍵情報に対応する装置固有鍵を持つ装置の装置ＩＤ情報も併せて記憶することが好ましい。

【００２１】かかる手段により、後日の記録番組データの視聴にあたって、装置ＩＤ情報および中間鍵ＩＤ情報を手掛かりに、再生・視聴する装置に対応し、かつ再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができる。

【００２２】次に前記デジタル衛星放送受信装置は、自らの装置ＩＤ情報およびあらかじめ相互利用が設定されている他の装置の装置ＩＤ情報を保持する手段と、装置が前記中間鍵情報を受信した場合に伴っている装置ＩＤ情報と前記装置内に保持している装置ＩＤ情報とを比較する装置ＩＤ比較手段と、前記装置ＩＤ比較手段において一致するものがあれば前記中間鍵情報記憶領域に前記中間鍵情報とその対応する装置ＩＤ情報とを合わせて記憶する手段とを備えることが好ましい。

【００２３】かかる構成により、あらかじめ設定されている他の装置を利用した後日での再生に備え、保持しておくべき中間鍵情報を判別し、中間鍵ＩＤ情報を対応付けて保持しておくことができる。

【００２４】次に前記デジタル衛星放送受信装置は、装置ＩＤ情報と中間鍵ＩＤ情報を手掛かりとして再生・視聴するデータに対応する中間鍵情報を記憶されている中間鍵ＩＤ情報の中から選択する中間鍵情報選択手段と、前記共通鍵情報とスクランブル番組データとを分離する共通鍵情報・スクランブル番組データ分離手段と、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えることが好ましい。

9

【００２５】かかる手段により、後日の記録番組データの視聴にあたって、装置ＩＤ情報および中間鍵ＩＤ情報を手掛かりに、再生・視聴する装置に対応し、かつ再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができ、その中間鍵から得た共通鍵を用いて、記録番組データのスクランブルを解除して再生・視聴することができる。

【００２６】上記目的を達成するために本発明に係るデジタル衛星放送受信装置は、多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を保持する装置固有鍵記憶手段と、前記受信したデータを中間鍵情報と共通鍵情報・スクランブル番組データとに分離する中間鍵情報フィルタと、前記分離した中間鍵情報を記憶する中間鍵情報記録手段と、前記分離された共通鍵情報・スクランブル番組データを記録する共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データ記録手段に対して前記記憶されている中間鍵情報を伝達し、共通鍵情報・スクランブル番組データとともに記録する中間鍵情報記録手段とを備える。

【００２７】かかる構成により、本発明に係るデジタル衛星放送受信装置は、多重化されて送られてくるデータから中間鍵情報をその他の共通鍵情報・スクランブル番組データから分離して有効な中間鍵情報を記憶し、番組データの記録時点で中間鍵情報を共通鍵情報・スクランブル番組データ記録手段に伝達して番組データと併せて記録することができる。

【００２８】次に前記デジタル衛星放送受信装置は、前記記録されている共通鍵情報・スクランブル番組データと中間鍵情報を読み出す記録データ読み出し手段と、前記読み出された共通鍵情報とスクランブル番組データを分離する共通鍵情報フィルタと、前記装置固有鍵と前記中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えることが好ましい。

【００２９】かかる構成により、中間鍵情報記憶手段により記憶されている中間鍵情報が更新された後であっても、スクランブル番組データと対応する中間鍵情報を利用することができ、番組データを再生することができる。

【００３０】次に前記デジタル衛星放送受信装置は、前記中間鍵情報記憶手段において、前記記録する装置が持つ装置固有鍵により復号される中間鍵情報のほか、他の装置に与えられた装置固有鍵により復号される中間鍵情報も併せて記憶することが好ましい。

【００３１】かかる手段により、視聴権利を持つ複数の

10

装置において、データを相互に再生・視聴ために必要な中間鍵を相互に持つことができる。

【００３２】次に前記デジタル衛星放送受信装置は、装置固有の装置ＩＤ情報を持ち、前記中間鍵情報記憶手段において、前記記憶する中間鍵情報に対応する装置固有鍵を持つ装置の装置ＩＤ情報も併せて記憶することが好ましい。

【００３３】かかる手段により、後日の記録番組データの視聴にあたって、装置ＩＤ情報を手掛かりとして、再生・視聴する装置に対応し、かつ再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができる。

【００３４】次に前記デジタル衛星放送受信装置は、自らの装置ＩＤ情報およびあらかじめ相互利用が設定されている他の装置の装置ＩＤ情報を保持する手段と、前記装置が前記中間鍵情報を受信した場合に伴っている装置ＩＤ情報と前記装置内に保持している装置ＩＤ情報とを比較する装置ＩＤ情報比較手段と、前記装置ＩＤ情報比較手段において一致するものがあれば前記中間鍵情報記憶領域に前記中間鍵情報とその対応する装置ＩＤ情報とを合わせて記憶する手段とを備えることが好ましい。

【００３５】かかる構成により、あらかじめ設定されている他の装置を利用した後日の再生に備え、保持しておくべき中間鍵情報を判別して保持しておくことができる。

【００３６】次に前記デジタル衛星放送受信装置は、装置ＩＤ情報を手掛かりとして再生・視聴するデータに対応する中間鍵情報を記憶されている中間鍵情報の中から選択する中間鍵情報選択手段と、前記共通鍵情報とスクランブル番組データを分離する共通鍵情報・スクランブル番組データ分離手段と、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えることが好ましい。

【００３７】かかる手段により、後日の記録番組データの視聴にあたって、装置ＩＤ情報を手掛かりに、再生・視聴する装置に対応し、かつ再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができ、その中間鍵から得た共通鍵を用いて、記録番組データのスクランブルを解除して再生・視聴することができる。

【００３８】次に前記デジタル衛星放送受信装置において、前記中間鍵情報および対応する中間鍵ＩＤ情報の記憶領域が、前記装置固有鍵を記憶している記憶領域がある記憶媒体と同じ記憶媒体内に設けられることが好ましい。

11

【００３９】さらに前記記憶媒体がＩＣカード記憶媒体であることが好ましい。

【００４０】かかる構成により、マスタ鍵を持つ記憶媒体が使用されているデジタル衛星放送受信装置に中間鍵情報および中間鍵ＩＤ情報が確実に記憶され、前記記憶媒体を他の装置に挿入してその装置をデジタル衛星放送受信装置として使用する場合などにおいても中間鍵情報が失われることなく、記録番組データの再生・視聴ができる。

【００４１】次に前記デジタル衛星放送受信装置において、前記中間鍵情報記憶領域が複数の記憶媒体にあり、１つは前記装置固有鍵の記憶領域がある記憶媒体の中に設けられ、他方は前記装置固有鍵の記憶領域がある記憶媒体とは別の記憶媒体に設けられることが好ましい。

【００４２】さらに前記記憶媒体がメモリカードであることが好ましい。

【００４３】かかる構成により、現行の中間鍵情報をマスタ鍵の記憶領域がある記憶媒体と同じ記憶媒体に記憶でき、かつ記録した番組データに対応する中間鍵情報および中間鍵ＩＤ情報をマスタ鍵のある記憶媒体とは別の記憶媒体に記憶させることができ、かかる中間鍵情報および中間鍵ＩＤ情報のみを分離することができる。

【００４４】次に前記デジタル衛星放送受信装置において、前記共通鍵情報・スクランブル番組データの記憶領域が装置に内蔵または外付けで接続された記憶媒体にあることが好ましい。

【００４５】さらに前記記憶媒体が磁気ディスク、内蔵メモリ、またはメモリカードであることが好ましい。

【００４６】かかる構成により、記録データの後日の再生・視聴にあたり、衛星デジタル受信装置内部で高速に記録データにアクセスできる。

【００４７】また前記デジタル衛星放送受信装置において、前記共通鍵情報・スクランブル番組データの記憶領域が可搬性を持った記憶媒体にあることが好ましい。

【００４８】さらに前記記憶媒体が磁気テープ、光磁気ディスク、ＤＶＤ（デジタルビデオディスク）、ＣＤ－Ｒ（追記型ＣＤ）、フォトＣＤまたはメモリカードであることが好ましい。

【００４９】かかる構成により、記録した放送番組データを可搬性あるものとでき、大量データの記録保存、他の衛星デジタル受信装置での利用に供することができる。

【００５０】

【発明の実施の形態】以下、本発明の実施形態について、図１および図８を用いて説明する。

【００５１】（実施の形態１）本実施形態１は、デジタル衛星放送の番組を記録した後、長期間が経過してもスクランブルを解除し視聴することを可能とするデジタル衛星放送受信装置である。本実施形態１は共通鍵暗号方式を利用した３重鍵構造の限定受信方式による衛星放送

12

システムを前提としており、暗号鍵は、マスタ鍵Ｋｍ、中間鍵たるワーク鍵Ｋｗ、番組データのデスクランブルを行なう共通鍵たるスクランブル鍵Ｋｓの３重の鍵からなり、ワーク鍵Ｋｗをマスタ鍵Ｋｍで暗号化した中間鍵情報を限定受信個別管理情報ＥＭＭ（Entitlement Management Message）とし、前記スクランブル鍵をワーク鍵で暗号化した共通鍵情報を限定受信共通情報ＥＣＭ（Entitlement Control Message）とする。以下、ＥＭＭの記憶、衛星デジタル番組データおよびＥＣＭの記録、記憶データの再生・視聴の３つの段階に分けて説明する。

【００５２】まず、ＥＭＭの記憶について示す。図１は本発明の第１の実施形態におけるデジタル衛星放送受信装置の構成図である。図１において、１０１はデジタル放送受信装置いわゆるセットトップボックス、１０２はデジタルＶＴＲなどの番組記憶装置、１０３は磁気テープなどの記録媒体、１０４はチューナと復調器から構成されるレシーバ・デモジュレータ、１０５はＭＰＥＧデコーダ、１０６はＭＰＥＧトランスポートデコーダ、１０７は限定受信を行うためのセキュリティモジュール、１０８はセキュリティモジュール内で限定受信管理を行うＩＣカード、１０９はスクランブルを解除するためのデスクランブラ、１１０はスクランブルを解除するために必要な鍵を含んだ情報である前記ＥＣＭおよびＥＭＭをＭＰＥＧトランスポートストリームから選択するためのＥＣＭ・ＥＭＭフィルタ、１１１はＭＰＥＧトランスポートストリーム入力切換回路、１１２はＩＣカード１０８内にあるＥＣＭ記憶領域、１１３はＩＣカード１０８内にあるＥＭＭ記憶領域である。なおＥＭＭはＥＭＭを特定するための中間鍵ＩＤ情報であるＥＭＭ－ＩＤが割り付けられてリスト形式で記憶されている。１１４はマスタ鍵Ｋｍの記憶領域である。また図示していないが装置を特定するためのの装置ＩＤ情報もＩＣカード１０８に記憶されている。

【００５３】本実施形態ではＥＭＭは衛星波に多重化されて送られてくる。まずスマートカード１０８にはあらかじめ装置ＩＤ情報とマスタ鍵Ｋｍが記憶されている。ＥＭＭは１か月に一度更新され、衛星波に多重化されて送信されるが、この際ＥＭＭは装置ＩＤ情報を伴って送信される。レシーバ・デモジュレータ１０４により受信されたデータはＭＰＥＧトランスポートストリーム入力切換回路１１１に送られる。ＭＰＥＧトランスポートストリーム入力切換回路１１１はＥＣＭ・ＥＭＭフィルタ１１０にデータを転送し、ＥＣＭ・ＥＭＭフィルタ１１０はデータからＥＭＭおよび装置ＩＤ情報をフィルタリングして抽出し、ＩＣカード１０８に送る。ＩＣカード１０８は送られてきた装置ＩＤ情報と保持している装置ＩＤ情報を比較し、一致すればＥＭＭをＥＭＭ記憶領域１１３に書き込み、一致しなければデータを破棄する。一致してＥＭＭを書き込む際には、ＥＭＭ－ＩＤを割り付けてＥＭＭとセットにしてＥＭＭ記憶領域１１３に格

13

納する。ここでＥＭＭは１か月に一度更新されるものとするが、ＥＭＭの記録にあたっては更新前のデータに上書きせず、来歴記録としてリスト形式で保存される。

【００５４】次にデジタル衛星放送の番組の記録について述べる。上記のＥＭＭの記憶方法で述べた通り、ＥＭＭは抽出され、ＥＣＭ・番組データと分離されている。ＥＣＭ・番組データはＥＣＭ・ＥＭＭフィルタによりフィルタリングされた後、記録手段たる番組記録装置１０２により記録される。番組記録装置１０２はデジタルビデオとし、その記録媒体１０３は磁気テープとする。その記録の際、ＥＣＭ・番組データの記憶領域のヘッダ領域に、ＥＭＭに対応付けられているＥＭＭ－ＩＤを記録する。

【００５５】次に記録番組データの再生について図２を使って説明する。図２の装置構成は図１に示した１０１のセットトップボックスから１１４のマスタ鍵Ｋｍ記憶領域まで同様である。再生したい番組データが記録されている記録媒体１０３を番組記録装置１０２にセットして再生する。番組記録装置１０２は記録媒体１０３からデータを読み出し、ＭＰＥＧトランスポートストリーム入力切換回路１１１に送る。ＭＰＥＧトランスポートストリーム入力切換回路１１１はＥＣＭ・ＥＭＭフィルタ１１０にデータを転送制御し、ＥＣＭ・ＥＭＭフィルタ１１０はデータからＥＣＭおよびヘッダにあるＥＭＭ－ＩＤをフィルタリングして抽出し、ＩＣカード１０８に送り、残りの番組データをデスクランブラ１０９に送る。スマートカード１０８はＥＣＭ・ＥＭＭフィルタ１１０から送られてきたＥＣＭをＥＣＭ記憶領域１１２に記憶する。ＩＣカード１０８は、さらに送られてきたＥＭＭ－ＩＤを手掛かりに、ＥＭＭ記憶領域１１３中のＥＭＭリストから一致するＥＭＭ－ＩＤが割り付けられているＥＭＭを選択する。次に、ＩＣカード１０８は選択されたＥＭＭをマスタ鍵Ｋｍにより復号し、中間鍵たるワーク鍵Ｋｗを得る。さらにＥＣＭをワーク鍵Ｋｗにより復号し、スクランブル鍵Ｋｓを得て、得られたＫｓをデスクランブラ１０９に送る。デスクランブラ１０９は番組データをＫｓにより復号し、スクランブルが解除されたデータをＭＰＥＧトランスポートデコーダ１０６に送る。データは最終的にＭＰＥＧデコーダ１０５によりＭＰＥＧ解凍され、モニタに映像データとして送られる。

【００５６】以上により、記録媒体１０３に記録された番組データを長期間経過後、ＥＭＭが更新された後においても再生・視聴することができる。

【００５７】なお、上記実施形態では番組記憶装置１０２は構成上、別筐体のビデオとしたが、内蔵されたものであってもよい。また記録媒体１０３として磁気テープとしたが、光磁気ディスク、ＣＤ－Ｒ（追記型ＣＤ）、フォトＣＤ、ＤＶＤ（デジタルビデオディスク）、メモリカードなど可搬性のある記録媒体であればよく、また

14

は可搬性がない記録媒体である内蔵もしくは外付のハード磁気ディスク装置、メモリなどの記録媒体であってもよい。

【００５８】また、ＥＭＭの更新期間を１か月としたが、運用により、別の周期で更新してもよい。例えば１週間に一度、番組ごとに１一度であってもよい。

【００５９】また、ＥＭＭとＥＭＭ－ＩＤの記録する際のデータ構造をリスト形式としたが、両者を対応付けて、過去の来歴を残せる限り、データの構造はリスト形式に限らなくともよい。

【００６０】また、ＥＭＭの送信は更新される度に１度衛星波による送信としたが、現行のＥＭＭが有効な期間においても複数回送信されるものであってもよい。

【００６１】（実施の形態２）実施形態２を図３を使って説明する。実施形態２はデジタル衛星放送の番組を記録したデータを後日、あらかじめ設定されている他の装置においても視聴ができる例である。実施形態１と同様、長期間が経過してもスクランブルを解除し視聴することを可能とする。実施形態１はＥＭＭが衛星波に多重化されて送られるものであったが、本実施形態ではＥＭＭの送信形態として電話回線を介した送信の例を挙げる。

【００６２】図３において、１０４は電話回線からデータを受信するモデムであるレシーバ・デモジュレータ、３１３は他のデジタル放送受信装置に対応するＥＭＭを記憶する第２ＥＭＭ記憶領域である。その他の構成１０１のセットトップボックスから１１４のマスタ鍵Ｋｍ記憶領域までは実施形態１に示したものと同様であり、説明を省略する。

【００６３】ＩＣカード１０８にはあらかじめマスタ鍵Ｋｍ、装置ＩＤ情報および相互利用が設定されている他の装置の装置ＩＤ情報が記憶されている。ＥＭＭは１か月に一度更新され、装置ＩＤ情報を伴って電話回線により送信される。レシーバ・デモジュレータ１０４により受信されたデータはＭＰＥＧトランスポートストリーム入力切換回路１１１に送られる。ＭＰＥＧトランスポートストリーム入力切換回路１１１はＥＣＭ・ＥＭＭフィルタ１１０にデータを転送し、ＥＣＭ・ＥＭＭフィルタ１１０はＥＭＭをフィルタリングして抽出し、ＩＣカード１０８に送る。ＩＣカード１０８は送られてきたＥＭＭに伴っている装置ＩＤ情報をＩＣカード１０８内にある自らの装置ＩＤ情報と比較し、一致する場合はＥＭＭ記憶領域１１３１１３に追記記憶する。一致しない場合は設定されている他の装置ＩＤ情報と比較し、ここで一致する場合は第２ＥＭＭ記憶領域３１３に追記記憶する。ＥＭＭを書き込む際には実施形態１同様、ＥＭＭにＥＭＭ－ＩＤを割り付けて、ＥＭＭと対応するＥＭＭ－ＩＤのセットとして格納・保持する。その際に更新前の情報には上書きせずに来歴記録として残しリスト形式で保持する。

15

【００６４】次にデジタル衛星放送の番組の記録について述べる。ＥＣＭ・番組データはＥＣＭ・ＥＭＭフィルタ１１０によりフィルタリングされた後、ＥＣＭ・番組データ記録手段たる番組記録装置１０２に送られ、記録される。その際、現行のＥＭＭをＥＭＭ記憶領域１１３から番組記憶装置１０２に伝達し、また現行の他の装置でのＥＭＭを第２ＥＭＭ記憶領域３１３から番組記憶装置１０２に伝達し、番組データのヘッダとして番組データとともに記憶する。番組記録装置１０２はデジタルビデオとし、その記録媒体１０３は磁気テープとする。その記録の際、ＥＣＭ・番組データの記憶領域のヘッダ領域に、それぞれのＥＭＭに対応付けられているＥＭＭ－ＩＤも記録する。

【００６５】次に番組データを記録した装置以外の他の装置での記録番組データの再生について図４を使って説明する。図４の装置構成は図１に示した１０１のセットトップボックスから１１４のマスタ鍵Ｋｍ記憶領域まで同様である。なお、装置にある装置ＩＤ情報を装置ＩＤ情報２とし、記録した装置の装置ＩＤ情報を装置ＩＤ情報２とする。まず再生したい番組データが記録されている記録媒体１０３を番組記録装置１０２にセットして再生する。番組記録装置１０２は記録媒体１０３からデータを読み出し、ＭＰＥＧトランスポートストリーム入力切換回路１１１に送る。ＭＰＥＧトランスポートストリーム入力切換回路１１１はＥＣＭ・ＥＭＭフィルタ１１０にデータを転送制御し、ＥＣＭ・ＥＭＭフィルタ１１０はデータからＥＣＭおよびヘッダにあるＥＭＭ－ＩＤと装置ＩＤ情報をフィルタリングして抽出し、ＩＣカード１０８に送り、残りの番組データをデスクランブラ１０９に送る。ＩＣカード１０８はＥＣＭ・ＥＭＭフィルタ１１０から送られてきたＥＣＭをＥＣＭ記憶領域１１２に記憶する。ＩＣカード１０８は、さらに送られてきたおよびＥＭＭ－ＩＤを手掛かりとしてＥＭＭ記憶領域１１３中のＥＭＭリストから一致する装置ＩＤ情報およびＥＭＭ－ＩＤが割り付けられているＥＭＭを選択する。次にＩＣカード１０８は選択されたＥＭＭをマスタ鍵Ｋｍにより復号し、中間鍵たるワーク鍵Ｋｗを得る。さらにＥＣＭをワーク鍵Ｋｗにより復号し、スクランブル鍵Ｋｓを得て、得られたスクランブル鍵Ｋｓをデスクランブラ１０９に送る。デスクランブラ１０９は番組データをＫｓにより復号し、スクランブルが解除されたデータをＭＰＥＧトランスポートデコーダ１０６に送る。データは最終的にＭＰＥＧデコーダ１０５によりＭＰＥＧ解凍され、モニタに映像データとして送られる。

【００６６】以上により、記録媒体１０３に記録された番組データを長期間経過後、ＥＭＭが更新された後、あらかじめ設定されている他の装置においても再生・視聴することができる。

【００６７】本実施形態ではＥＭＭの更新期間を１か月としたが、運用により、別の周期で更新してもよい。例

16

えば１週間に一度、番組ごとに１一度であってもよい。

【００６８】また、ＥＭＭと装置ＩＤ情報およびＥＭＭ－ＩＤの記録する際のデータ構造をリスト形式としたが、両者を対応付けて、過去の来歴を残せる限り、データの構造はリスト形式に限らなくともよい。

【００６９】また、ＥＭＭの送信は更新される度に１度電話回線による送信としたが、現行のＥＭＭが有効な期間においても複数回送信されるものであってもよい。また実施形態１に示したように衛星波に多重化されて送信される場合も同様に考えることができる。

【００７０】（実施形態３）実施形態３を図５を使って説明する。実施形態３も実施形態１または２と同様、デジタル衛星放送の番組を記録した後、長期間が経過してもスクランブルを解除し視聴することを可能とするデジタル衛星放送受信装置であり、共通鍵暗号方式を利用した３重鍵構造の限定受信方式による衛星放送システムを前提とする点も同様である。本実施形態ではＥＭＭ記憶領域が２つあり、図５において、１１３はＥＭＭ記憶領域の１つであり、５１３は他方のＥＭＭ記憶領域である。その他の構成は実施形態１に示したものと同じであり、構成の説明は省略する。本実施形態では実施形態１と同様、ＥＭＭは衛星波に多重化されて送信されるものとする。送信されるＥＭＭは実施形態１と同様、装置ＩＤ情報を伴って送信される。レシーバ・デモジュレータ１０４により受信されたデータはＭＰＥＧトランスポートストリーム入力切換回路１１１に送られる。ＭＰＥＧトランスポートストリーム入力切換回路１１１はＥＣＭ・ＥＭＭフィルタ１１０にデータを転送し、ＥＣＭ・ＥＭＭフィルタ１１０はデータからＥＭＭおよび装置ＩＤ情報をフィルタリングして抽出し、ＩＣカード１０８に送る。ＩＣカード１０８は送られてきた装置ＩＤ情報と保持している装置ＩＤ情報を比較し、一致すればＥＭＭをＥＭＭ記憶領域１１３および５１３両方に書き込み、一致しなければデータを破棄する。一致してＥＭＭを書き込む際には、ＥＭＭ－ＩＤを割り付けてＥＭＭとセットとしてＥＭＭ記憶領域１１３および５１３に格納する。ここでＥＭＭは１か月に一度更新されるものとするが、前記ＥＭＭの記録にあたりＥＭＭ記憶領域１１３では更新前のデータに上書きし、常に現行のＥＭＭを記憶する。一方ＥＭＭ記憶領域５１３においては更新前のデータに上書きせず、過去のＥＭＭ情報およびＥＭＭ－ＩＤを来歴記録としてリスト形式で保存する。

【００７１】次に記録番組データの再生について図６を使って説明する。図６の装置構成は図５に示した１０１のセットトップボックスから１１４のマスタ鍵Ｋｍ記憶領域まで同様である。まず再生したい番組データが記録されている記録媒体１０３を番組記録装置１０２にセットして再生する。番組記録装置１０２は記録媒体１０３からデータを読み出し、ＭＰＥＧトランスポートストリーム入力切換回路１１１に送る。ＭＰＥＧトランスポー

17

トストリーム入力切換回路１１１はＥＣＭ・ＥＭＭフィルタ１１０にデータを転送制御し、ＥＣＭ・ＥＭＭフィルタ１１０はデータからＥＣＭおよびヘッダにあるＥＭＭ－ＩＤと装置ＩＤ情報をフィルタリングして抽出し、ＩＣカード１０８に送り、残りの番組データをデスクランブラ１０９に送る。ＩＣカード１０８はＥＣＭ・ＥＭＭフィルタ１１０から送られてきたＥＣＭをＥＣＭ記憶領域１１２に記憶する。ＩＣカード１０８は、さらに送られてきたおよびＥＭＭ－ＩＤを手掛かりに、ＥＭＭ記憶領域１１３および５１３中のＥＭＭリストから一致する装置ＩＤ情報およびＥＭＭ－ＩＤが割り付けられているＥＭＭを選択する。ＥＭＭ記憶領域５１３中のＥＭＭリスト中に該当するＥＭＭがある場合にはＥＭＭ記憶領域５１３からＩＣカード１０８にそのＥＭＭを送信する。次に、ＩＣカード１０８は選択されたＥＭＭをマスタ鍵Ｋｍにより復号し、中間鍵たるワーク鍵Ｋｗを得る。さらにＥＣＭをワーク鍵Ｋｗにより復号し、スクランブル鍵Ｋｓを得て、得られたスクランブル鍵Ｋｓをデスクランブラ１０９に送る。デスクランブラ１０９は番組データをスクランブル鍵Ｋｓにより復号し、スクランブルが解除されたデータをＭＰＥＧトランスポートデコーダ１０６に送る。データは最終的にＭＰＥＧデコーダ１０５によりＭＰＥＧ解凍され、モニタに映像データとして送られる。

【００７２】以上により、記録媒体１０３に記録された番組データを長期間経過後、ＥＭＭが更新された後、再生・視聴することができる。

【００７３】なお、本実施形態では、ＥＭＭ記憶領域５１３をビデオ装置内のメモリとしたが、セットトップボックス１０１内に記憶領域を設けてもよい。またＥＣＭ・番組データ記憶媒体内にあってもよく、内蔵ハードディスク、大容量のメモリなどが挙げられる。またＥＭＭ記憶領域５１３を可搬性のある記憶媒体である磁気テープ、ＣＤ－Ｒ、ＤＶＤなどの記憶媒体に設けることも可能であり、その場合はＥＭＭ記憶領域５１３をＥＣＭ・番組データ記憶領域のヘッダ領域に設ける構成がある。

【００７４】（実施形態４）実施形態４を図７を使って説明する。実施形態４も実施形態１または２と同様、デジタル衛星放送の番組を記録した後、長期間が経過してもスクランブルを解除し視聴することを可能とするデジタル衛星放送受信装置であり、共通鍵暗号方式を利用した３重鍵構造の限定受信方式による衛星放送システムを前提とする点も同様である。また図７において、装置の構成１０１のセットトップボックスから１１４のマスタ鍵Ｋｍ記憶領域までは実施形態１または２に示したものと同様であり、ここでは説明を省略する。さらにＥＭＭの記憶において実施形態１または２におけるＥＭＭの記憶と同様でよく、ＥＭＭの更新も実施形態１または２と同様に月に１度とする。ただし、本実施形態ではＥＭＭ－ＩＤは必ずしも必要ではなく、ＥＭＭ記憶領域１１３

18

には現行のＥＭＭのみが記憶されている。

【００７５】次にデジタル衛星放送の番組の記録について述べる。レシーバ・デモジュレータ１０４に受信された衛星波のデータはＥＣＭ・ＥＭＭフィルタ１１０によりフィルタリングされた後、記録手段たる番組記録装置１０２により記録される。番組記録装置１０２はデジタルビデオとし、その記録媒体１０３は磁気テープとする。その記録の際、ＥＭＭ記憶領域１１３に記憶されているＥＭＭが前記番組記録装置１０２に伝達され、番組記録装置１０２は、ＥＣＭ・番組データの記憶領域のヘッダ領域に、伝達されたＥＭＭを記録する。このように記録媒体１０３にはＥＣＭ・番組データとそれに対応するＥＭＭがセットで記録され、ＥＭＭが後に更新され、ＥＭＭ記憶領域１１３に記憶されている現行ＥＭＭが変わった場合でも番組データの再生に必要なＥＭＭは失われない。

【００７６】次に記録番組データの再生について図８を使って説明する。図８の装置構成は図７に示した１０１のセットトップボックスから１１４のマスタ鍵Ｋｍ記憶領域まで同様である。再生したい番組データが記録されている記録媒体１０３を番組記録装置１０２にセットして再生する。番組記録装置１０２は記録媒体１０３からデータを読み出し、ＭＰＥＧトランスポートストリーム入力切換回路１１１に送る。ＭＰＥＧトランスポートストリーム入力切換回路１１１はＥＣＭ・ＥＭＭフィルタ１１０にデータを転送制御し、ＥＣＭ・ＥＭＭフィルタ１１０はデータからＥＭＭおよびＥＣＭをフィルタリングして抽出し、ＩＣカード１０８に送り、残りの番組データをデスクランブラ１０９に送る。ＩＣカード１０８はＥＣＭ・ＥＭＭフィルタ１１０から送られてきたＥＣＭをＥＣＭ記憶領域１１２に記憶し、ＥＭＭをＥＭＭ記憶領域１１３に記憶する。この際、データ再生の前にＥＭＭ記憶領域１１３に格納されていた現行のＥＭＭを上書きせずに一時的に退避させ、データ再生のために取り込んだＥＭＭを再生用の一時利用のＥＭＭとして使用する。次に、ＩＣカード１０８は前記再生用ＥＭＭをマスタ鍵Ｋｍにより復号し、中間鍵たるワーク鍵Ｋｗを得る。さらにＥＣＭをワーク鍵Ｋｗにより復号し、スクランブル鍵Ｋｓを得て、得られたＫｓをデスクランブラ１０９に送る。デスクランブラ１０９は番組データをＫｓにより復号し、スクランブルが解除されたデータをＭＰＥＧトランスポートデコーダ１０６に送る。データは最終的にＭＰＥＧデコーダ１０５によりＭＰＥＧ解凍され、モニタに映像データとして送られる。

【００７７】以上により、記録媒体１０３に記録された番組データを長期間経過後、ＥＭＭが更新された後においても再生・視聴することができる。

【００７８】なお、上記実施形態では番組記憶装置１０２は構成上、別筐体のビデオとしたが、内蔵されたものであってもよい。また記録媒体１０３として磁気テープ

19

としたが、光磁気ディスク、ＣＤ－Ｒ（追記型ＣＤ）、フォトＣＤ、ＤＶＤ、メモリカードなど可搬性のある記録媒体であればよく、または可搬性がない記録媒体である内蔵もしくは外付のハード磁気ディスク装置、メモリなどの記録媒体であってもよい。

【００７９】また、ＥＭＭの更新期間を１か月としたが、運用により、別の周期で更新してもよい。例えば１週間に一度、番組ごとに１一度であってもよい。

【００８０】また、ＥＭＭの送信は更新される度に１度衛星波による送信としたが、現行のＥＭＭが有効な期間においても複数回送信されるものであってもよい。

【００８１】

【発明の効果】以上のように本発明によれば番組を記録した後、長期間が経過してＥＭＭが更新された場合でも、記録番組データのスクランブルを解除し、視聴が可能となり、また記録に用いたデジタル放送受信装置とは異なる他のデジタル衛星放送受信装置で再生した場合でも同様に記録番組データのスクランブルを解除し、視聴することが可能となる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るデジタル放送受信装置の構成図

【図２】本発明の第１の実施形態に係るデジタル放送受信装置の構成図

【図３】本発明の第２の実施形態に係るデジタル放送受信装置の構成図

【図４】本発明の第２の実施形態に係るデジタル放送受信装置の構成図

【図５】本発明の第３の実施形態に係るデジタル放送受信装置の構成図

20

【図６】本発明の第３の実施形態におけるデジタル放送受信装置の構成図

【図７】本発明の第４の実施形態におけるデジタル放送受信装置の構成図

【図８】本発明の第４の実施形態におけるデジタル放送受信装置の構成図

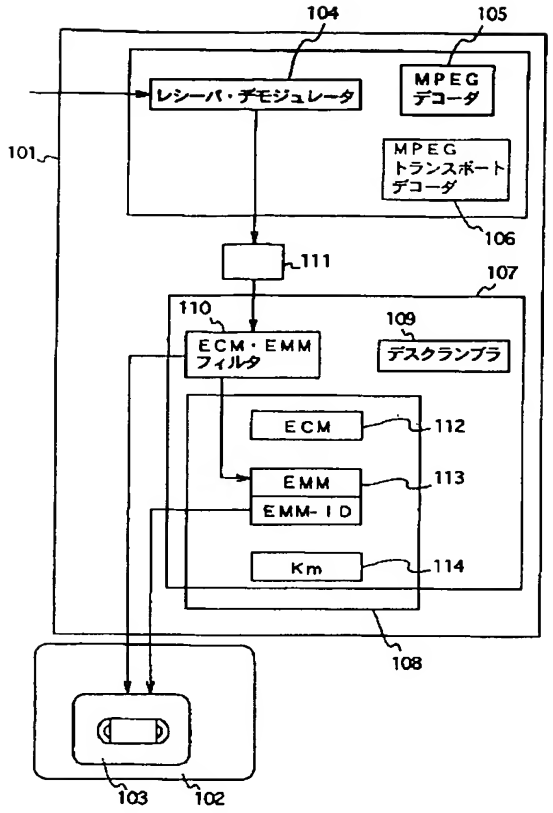
【図９】従来の技術によるデジタル放送受信装置の構成図

【図１０】従来の技術によるデジタル放送受信装置の構成図

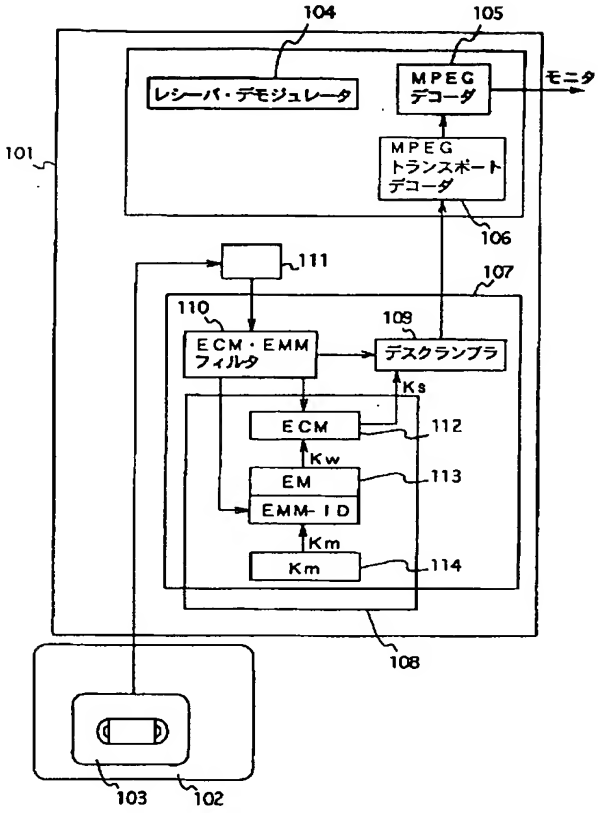
【符号の説明】

１０１，９０１　ディジタル放送受信装置
１０２，９０２　番組記録装置
１０３，９０３　記録媒体
１０４，９０４　レシーバ・デモジュレータ
１０５，９０５　ＭＰＥＧデコーダ
１０６，９０６　ＭＰＥＧトランスポートデコーダ
１０７，９０７　セキュリティーモジュール
１０８，９０８　ＩＣカード
１０９，９０９　デスクランブラ
１１０，９１０　ＥＣＭ・ＥＭＭフィルタ
１１１，９１１　ＭＰＥＧトランスポートストリーム入力切換回路
１１２，９１２　ＥＣＭ記憶領域
１１３，５１３，９１３　ＥＭＭ記憶領域
１１４，９１４　マスタ鍵Ｋｍ記憶領域
３１３　第２ＥＭＭ記憶領域

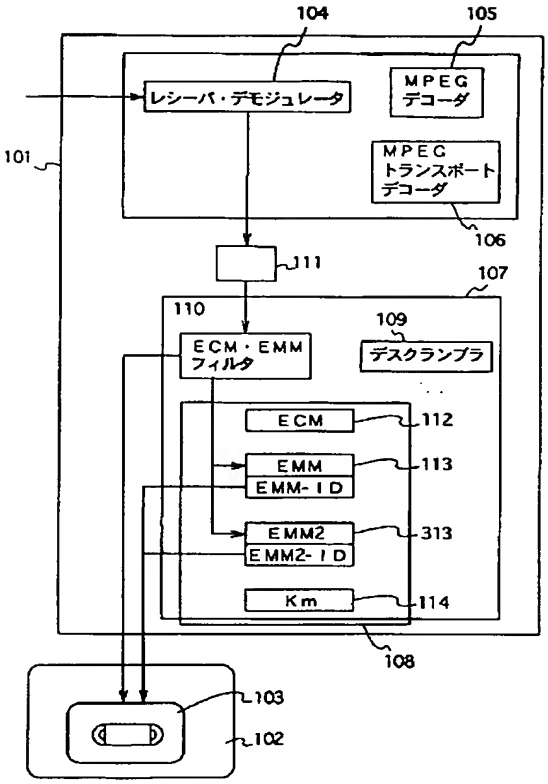
【図１】


104
105
レシーバ・デモジュレータ
MPEG
デコーダ
MPEG
トランスポート
デコーダ
101
106
111
107
110
109
ECM・EMM
フィルタ
デスクランブラ
ECM
112
EMM
113
EMM-ID
Km
114
108
103
102

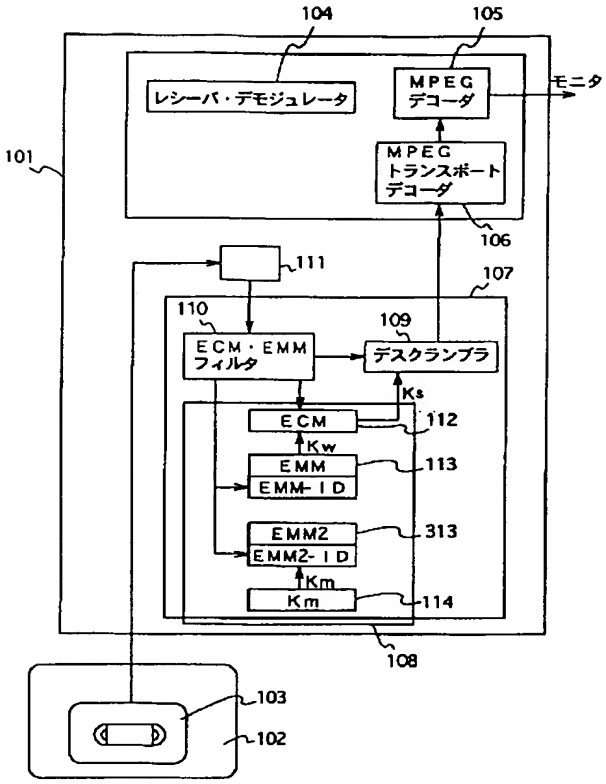
【図２】


104
105
レシーバ・デモジュレータ
MPEG
デコーダ
モニタ
MPEG
トランスポート
デコーダ
101
106
111
107
110
108
ECM・EMM
フィルタ
デスクランブラ
Ks
ECM
112
Kw
EM
113
EMM-ID
Km
Km
114
108
103
102

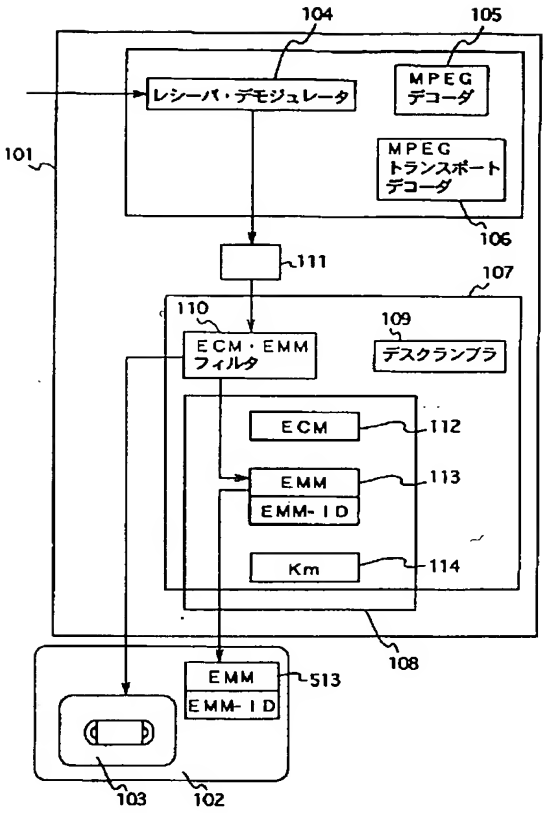
【図３】


104
105
レシーバ・デモジュレータ
MPEG
デコーダ
MPEG
トランスポート
デコーダ
101
106
111
107
110
109
ECM・EMM
フィルタ
デスクランブラ
ECM
112
EMM
EMM-ID
113
EMM2
EMM2-ID
313
Km
114
108
103
102

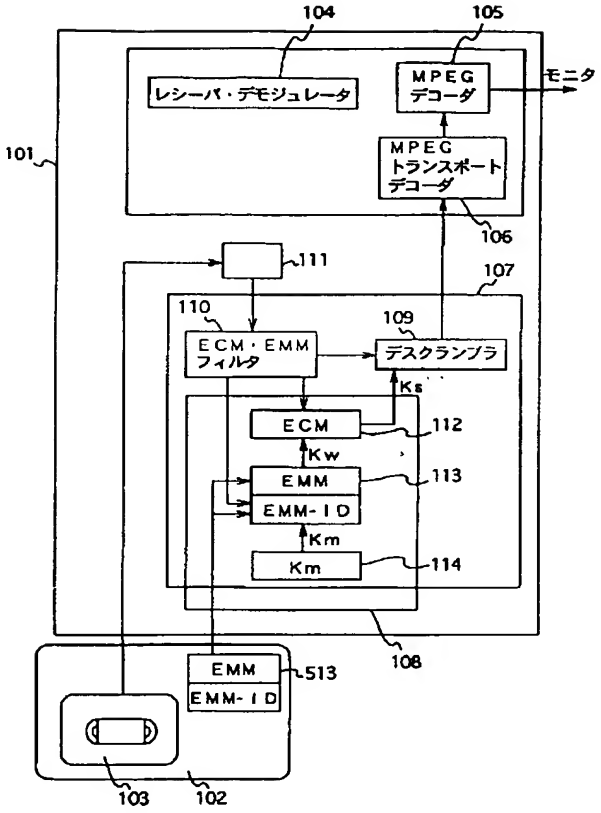
【図４】


104
105
レシーバ・デモジュレータ
MPEG
デコーダ
モニタ
MPEG
トランスポート
デコーダ
101
106
111
107
110
109
ECM・EMM
フィルタ
デスクランブラ
Ks
ECM
112
Kw
EMM
EMM-ID
113
EMM2
EMM2-ID
313
Km
Km
114
108
103
102

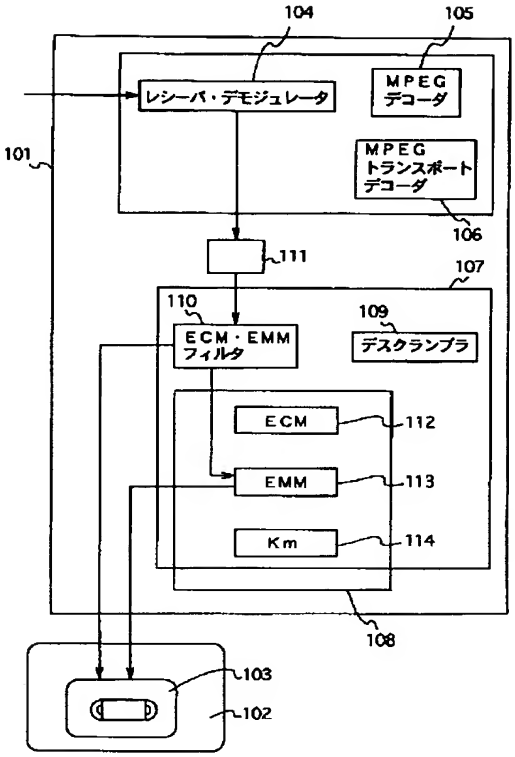
【図５】


104
105
レシーバ・デモジュレータ
MPEG
デコーダ
MPEG
トランスポート
デコーダ
101
106
111
107
110
109
ECM・EMM
フィルタ
デスクランブラ
ECM
112
EMM
113
EMM-ID
Km
114
108
EMM
513
EMM-ID
103
102

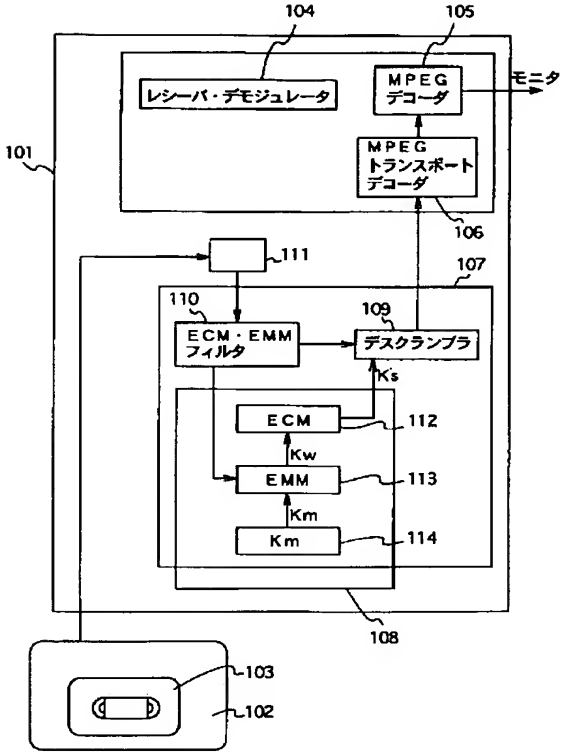
【図６】


104
105
レシーバ・デモジュレータ
MPEG
デコーダ
モニタ
MPEG
トランスポート
デコーダ
101
106
111
107
110
109
ECM・EMM
フィルタ
デスクランブラ
Ks
ECM
112
Kw
EMM
113
EMM-ID
Km
Km
114
108
EMM
513
EMM-ID
103
102

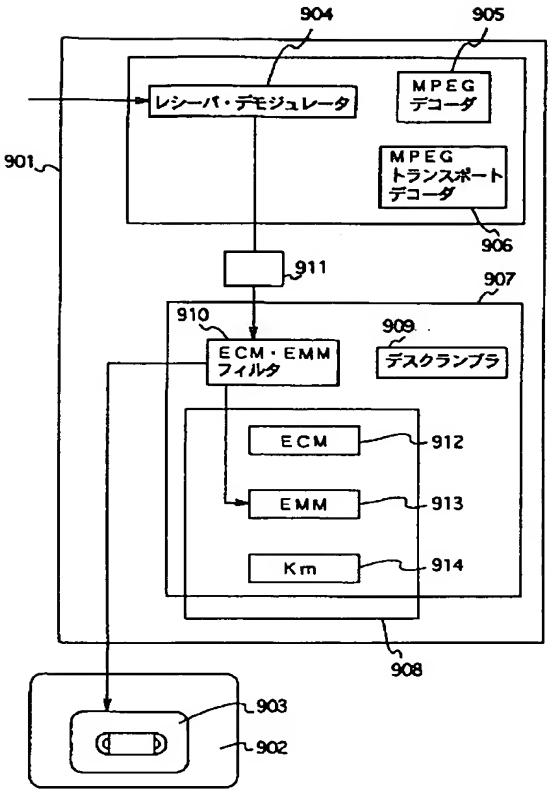
【図７】


104
105
レシーバ・デモジュレータ
MPEG
デコーダ
MPEG
トランスポート
デコーダ
101
106
111
107
110
109
ECM・EMM
フィルタ
デスクランブラ
ECM
112
EMM
113
Km
114
108
103
102

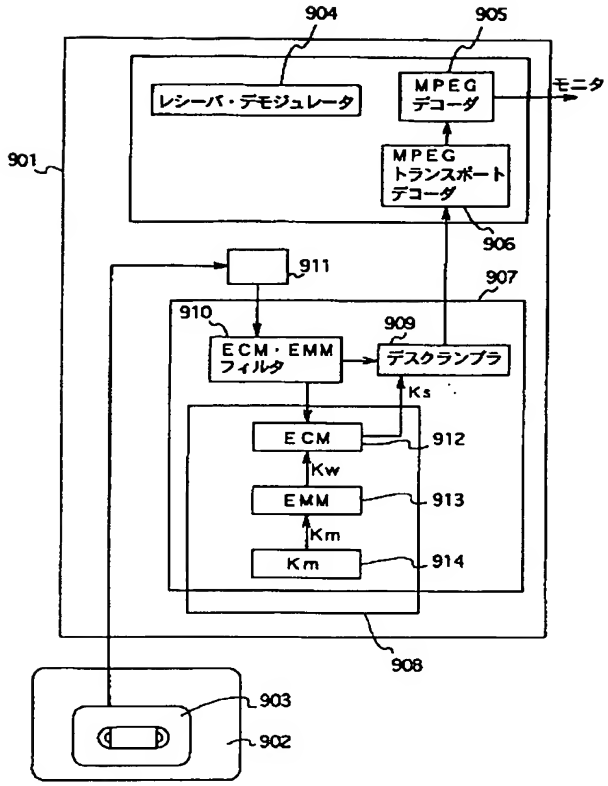
【図８】


104
105
レシーバ・デモジュレータ
MPEG
デコーダ
モニタ
MPEG
トランスポート
デコーダ
101
106
111
107
110
109
ECM・EMM
フィルタ
デスクランブラ
Ks
ECM
112
Kw
EMM
113
Km
Km
114
108
103
102

【図９】



【図１０】



フロントページの続き

(51) Int. Cl.[6]	識別記号	F I	
H04N 5/91		H04N 5/91	Z